PAR PUBLIC ADMINISTRATION REVIEW

Karen Renaud
Abertay University
Rhodes University
Craig Orgeron
Mississippi Department of Information Technology Services

Merrill Warkentin
P. Edward French
Mississippi State University

Research Article

Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China

Abstract: *Governments can intervene to a greater or lesser extent in managing the risks that citizens face. They can adopt a maximal intervention approach (e.g., COVID-19) or a hands-off approach (e.g., unemployment), effectively "responsibilizing" their citizens. To manage the cyber risk, governments publish cyber-related policies. This article examines the intervention stances the governments adopt in supporting individual citizens managing their personal cyber risk. The authors pinpoint the cyber-related responsibilities that several governments espouse, applying a "responsibilization" analysis. Those applying to citizens are identified, thereby revealing the governments' cyber-related intervention stances. The analysis reveals that most governments adopt a minimal cyber-related intervention stance in supporting their citizens. Given the increasing number of successful cyber attacks on individuals, it seems time for the consequences of this stance to be acknowledged and reconsidered. The authors argue that governments should support individual citizens more effectively in dealing with cyber threats.*

Evidence for Practice

- National cyber security policies assign a range of responsibilities for cyber security actions to different stakeholders.
- Governments embrace and accept responsibilities ranging from dealing with cyber criminals and protecting government assets to strengthening international collaboration with other countries.
- When it comes to individual citizens, the Five Eyes governments (United Kingdom, United States, Canada, Australia, and New Zealand) generally offer advice and related services and then relegate the task of managing cyber attacks to individual citizens. They offer very little direct support, in stark contrast with the range of services and funding offered to businesses and to support research.

The huge advantages that global citizens gain from being online are somewhat clouded by the significant risks they are exposed to while utilizing online services (de Bruijn and Janssen 2017). Cyber attacks have become an everyday occurrence, with cyber criminals even exploiting pandemics to attack people worldwide (Gatlan 2020). During February 2020, for example, a total of 623 million data records were breached during cyber attacks (Irwin 2020). In 2018, the World Economic Forum ranked cyber attacks third in worldwide threats (World Economic Forum 2018).

Cyber criminals may target nations or societies (such as interference with elections), organizations (such as the Sony and Stuxnet attacks), or individuals (i.e., private internet users or "netizens"; see Zhu, Huang, and Zhang 2019). Citizens experience malicious assaults on their information security in the form of phishing attempts, malware, malicious state actors, and the actions of other motivated and resourceful individuals who seek to steal or corrupt their information or to defraud them (Nichols 2019; Xavier and Pati 2012).

Organizations and governments deploy a range of technical tools to improve their own cyber security and to repel attacks, and they allocate significant funds to this activity (Singh et al. 2013). Yet Norris, Joshi, and Finin (2015) point out that the major problem is actually humans in the system making mistakes or omissions, thereby unwittingly aiding cyber attackers. Governments and organizations can, and do, employ professionals to deliver regular security training to their employees, and information technology (IT) staff provide advice and assist in recovery from incidents. Individual citizens, on the other hand, seldom have access to this kind of expert training or funding, nor do they necessarily even realize that they are at risk (Mustafa and Kar 2019; Nthala and Flechais 2017). This means that citizens across the globe are particularly vulnerable, as soft targets fall victim to devastating cyber attacks (ABC7 Chicago 2017; Hughes 2020; Kubiak 2020; Nichols 2019; Selby 2019; Wang 2018; WTVR 2019).

Karen Renaud is a Scottish computing scientist and Fulbright alumni working on all aspects of human-centered security and privacy. She is visiting professor at Rhodes University in South Africa and Professor Extraordinaire at the University of South Africa. Her research approach is multidisciplinary, learning from other more established fields and applying methods and techniques from other disciplines to cyber security. She is associate editor of the *International Journal of Human Computer Studies*, *Transactions on Computer Forensics and Security*, *Information Technology & People*, and the *Journal of Intellectual Capital*.
Email: k.renaud@abertay.ac.uk

Craig Orgeron is executive director of the Mississippi Department of Information Technology Services and chief information officer for the State of Mississippi. He has extensive information technology experience in both the private sector and the federal and state levels of the public sector. He has served as president of the National Association of State Chief Information Officers and as a member of the Executive Committee of the Multi-State Information Sharing & Analysis Center.
Email: Craig.Orgeron@its.ms.gov

Merrill Warkentin is William L. Giles Distinguished Professor at Mississippi State University, where he serves as the James J. Rouse Endowed Professor of Information Systems in the College of Business. His primary research focus is behavioral information system security and privacy issues. His research has appeared in *MIS Quarterly*, *Government Information Quarterly*, the *Journal of MIS*, the *Journal of the AIS*, and other leading journals. He was named an ACM Distinguished Scientist in 2018. He holds or has held editorial positions at many leading information systems journals.
Email: m.warkentin@msstate.edu

P. Edward French is department head and professor in the Department of Political Science and Public Administration at Mississippi State University. He specializes in human resource management, politics of state and local governments, and comparative public administration. His work has been published in numerous academic outlets. He is former editor in chief of *Public Personnel Management* and currently serves as an associate editor of *Public Administration Review*.
Email: efrench@pspa.msstate.edu

Public Administration Review, Vol. 80, Iss. 4, pp. 577–589. © 2020 The Authors. *Public Administration Review* published by Wiley Periodicals LLC on behalf of The American Society for Public Administration.
DOI: 10.1111/puar.13210.

Nye (2011), in contemplating the lessons that the nuclear industry has for the cyber security field, makes the point that both fields suffer from the fact that civilian uses complicate national security strategies. As mentioned before, average citizens might well leave themselves open to attack out of ignorance, fear, or a lack of requisite skills. There are a number of ways that governments can address this kind of situation. Their actions can range from strongly interventionist, whereby they legislate specific actions and punish noncompliance, to relatively hands-off provision of advice. There are also gradations between these two extremes, but the hands-off approach is often referred to as *responsibilization* of citizens. Shamir (2018, 4) writes that responsibilization is "a call for action; an interpellation which constructs and assumes a moral agency and certain dispositions to social action that necessarily follows."

In considering this question for a range of *noncyber* issues, Tsinovoi and Adler-Nissen (2018, 3) explain that "the 'duty of care' earlier embraced by many governments has now been supplanted with a mind-set of 'citizens as resources.'" Whereas governments previously sought to act as shepherds protecting their flocks, with citizens being passive recipients of such protection, citizens in neoliberal-led countries, in particular, are now seen as active forces to be mobilized to take care of themselves—that is, *responsibilized*. Instead of embracing their erstwhile duty of care, governments now focus on building capabilities (Tsinovoi and Adler-Nissen 2018). Responsibilization can be seen as a reduction of direct government intervention with respect to a particular issue, trending toward less intervention, with gradations similar to those suggested by Assaf (2008). For matters that governments judge merit minimal intervention, responsibilized citizens are provided with advice and perhaps on-demand services and then are expected to take full responsibility for managing those matters. They subsequently face the consequences if they do not follow the government's advice.

This responsibilization concept was first mentioned in relation to cyber security in an article by Harknett and Stever (2009), in which they offer analysis of federal reorganization attempts juxtaposing recent advances in technology to those of nuclear technology. The authors call for "cybersecurity to rest on a balanced triad of intergovernmental relations, private corporate involvement, and active cyber citizenship as a resilient model that can manage this new and challenging security environment" (Harknett and Stever 2009, 1).

Building on these foundational efforts, this article seeks to reveal the extent to which citizens of selected countries are being responsibilized when it comes to cyber security—that is, what level of intervention is envisaged by the governments in question. In this article, we investigate six governments' intervention stances in terms of supporting their citizens in the cyber realm.

We analyzed the six countries' cyber security strategy policies, seeking to highlight the implicit intervention stances that inform cyber threat management within the policies. Policies are indeed a viable artifact to analyze, because, as Väljataga (2018) argues, "National cyber security strategies serve as useful tool to identify a state's general position in regard to the rules and principles in cyberspace." To extract responsibilities from statements in policies, we utilized the problematization approach formulated by Bacchi (2009, 2012). We then classified each responsibility with respect to how it reflects the specific government's intervention stance, using Assaf's (2008) intervention categorization.

In the next section, we review the evolution of cyber policy in public administration to contextualize our research. We then explain how we used Bacchi's problematization approach to formulate a set of responsibilization questions to guide this research. We report on each step and conclude that citizens are generally responsibilized to manage their own cyber protection by the Five Eyes countries (United Kingdom, United States, Canada, Australia, and New Zealand), while China exercises more monitoring of individual behaviors. The implicit assumption by the Five Eyes countries appears to be that their citizens will be able to resist cyber threats without direct support, if only enough advice and guidance is provided. In effect, these governments fully responsibilize their citizens in dealing with cyber security threats.

We conclude the article by suggesting that the implicit assumption underlying this responsibilization of citizens is, in fact, misguided. We argue that the Five Eyes governments ought to rethink their cyber responsibilization stance.

Cyber Policy in Public Administration

Beginning with the early work of Kraemer and Dutton (1978), and since the publication in 1986 of a special issue of *Public Administration Review* about public management information systems, both academics and practitioners have focused on the impact of IT in the public sector arena (Bretschneider 1990; Caudle 1990; Northrop et al. 1990). Early work sought insights into the use of IT by government agencies for internal operational needs (Nedovic-Budic and Godschalk 1996; Norris and Kraemer 1996; Ventura 1995).

E-Government Emergence

As time progressed, the birth and rapid expansion of the internet prompted a research focus on electronic government (e-government) as a newly emergent platform enabling governments across the globe to deliver cost-effective and convenient services to citizens, private sector organizations, employees, and other nongovernmental agencies (Ho 2002; Moon 2002; Norris and Jae Moon 2005; West 2004). As e-government became more firmly established, scholars pursued both descriptive and comparative research, focusing on models and rates of adoption, as well as evaluating service value and user approval (Coursey and Norris 2008; Lee, Chang, and Berry 2011; Norris and Reddick 2013). Over recent years, the culture of innovation that IT fostered in the public sector (Desouza and Bhagwatwar 2012) has generated fresh avenues of study centered on the expansive growth of social media.

The Dark Side of the Internet

The rise of the internet, and of a truly worldwide user community, has ushered in an era of unanticipated societal risks with an ever-expanding set of interactive tools utilized to advance electronic transactions (AlDairi and Tawalbeh 2017; Andreasson 2011; Cordes 2010; Goodyear et al. 2010; Harknett and Stever 2011; Zhao and Zhao 2010). This vast and evolving expanse of technology connectivity has paved the way for cyber attacks to become a contemporary reality for citizens across the globe

(Parshall 2018). Moreover, several concerns have been raised over privacy violations (Caruson, MacManus, and McPhee 2012).

Cyber Security Challenge

Cyber security has become a complex and vexing challenge of the twenty-first century (Harknett and Stever 2011), with governments often under almost continual cyber attack (Norris et al. 2019). De Bruijn and Janssen (2017, 1) note that "interest in cyber security issues often focuses on incidents and how to deal with them after the fact, while a concern for prevention and investments in better cyber security have lagged behind." The rapid rise of cyber security, as a global issue, has buttressed the argument for the protection of corporations and individuals from the untoward use of the internet by illicit actors. Authors and academics have, in recent years, called for multistakeholder internet governance (Kuehn 2014), given the rising concern for national security as a key consideration in the formulation of public policy. Evolving and advancing cyber security challenges persist and plague nations and individual citizens. The governance of cyber security is fixed as a crucial element contributing to the security of a nation (Christensen and Petersen 2017; Hathaway and Stewart 2014; Kello 2013). Kuerbis and Badiei (2017) note that the governance of cyber security is disposed to nationalization, described as a mingling of homeland and societal cyber security.

Cyber Security Policy

Cyber security policy has become inextricably linked to internet governance, and, as argued by Mueller (2017), cyber security–centric dialogue has come to overshadow the advance of internet governance. While advancing the notion that national and societal cyber security should be differentiated, Mueller (2017) argues equally for an interlocking compatibility. Crucial in the quickening development of policy and governance models for both cyber security and the internet is the coercive potential of illicit actors and the interstate power shifts inherent in the modern global information age (Nye 2015). The intersection of unprecedented technological advances, politics, and national security concerns has fueled intense deliberation regarding the suitable responsibility of nation-states in both international cyber security policy and internet governance (Shackelford and Craig 2014).

Collaboration and Cooperation

Over the last two decades, it has become clear that intergovernmental and interjurisdictional cooperation is required to address society's most pressing threats, such as counterterrorism (Kincaid and Cole 2002). Elazar (1990) proposed a blended concept of cooperation and coercion that offers a framework for describing the nature and pattern of this type of intergovernmental relations. Under such circumstances, the center of policy responsibility, authority, and power may shift from state and local governments to the national government, and a pattern of regulatory (coercive) intergovernmental relations may transpire (Cho and Wright 2004). Cyber security policy and internet governance as offensive measures to protect a nation and its citizens and businesses from cyber risks may substantiate a highly federalized system yet still compel an intergovernmentalized strategy to minimize harm and disruption. While the debate as to whether these intergovernmental relations regarding cyber security should be cooperative, coercive, or a convergence of the two, is beyond the scope of this research. The implications for initiatives and changes these may impose on the federal system certainly warrant exploration in future study.

While individual nations have developed and circulated unique national cyber security strategies, which vary in domestic focal points and methods (Luiijf, Besseling, and de Graaf 2013), numerous countries and international bodies have also pursued common ground, forging mutual obligations on cyber security through the Draft International Code of Conduct for Information Security (Lkhagvasuren 2017).

Cyber Power

Even with efforts to develop cyber security policy and governance across a myriad of sectors, the academic literature addressing governance constructs is limited.[1] Cyber power as a contextual model (Christou 2017) is rooted in the pragmatic need to safeguard technology and telecommunication assets from the rising tide of global cyber risks (Senol 2017). This continually expanding information and communication infrastructure, often privately owned and operated (Carr 2016; Farrand and Carrapico 2018), provides a vast array of electronic services and transactions and has become a potent force in cyber warfare (Senol 2017).

Cyber security policy development is firmly coupled with the securing of critical technology infrastructure, often affecting nation-state power dispersement (Valeriano and Maness 2018), as well as inciting rivalry for economic gain and influence over all aspects of the internet (Hathaway 2014). With the contextual underpinning of cyber power, the safeguarding of cyber space and the mitigation of cyber risk have become top security priorities for nations globally, with policy focus in three arenas: cyber crime, critical information infrastructures, and cyber defense (Farrand and Carrapico 2018). Cyber power, as a predominant ingredient in cyber security policy development, informs views on the propensity for cyber war, with the internet once again the focal point of nationalistic power struggles (Gartzke 2013; Glaser and Kaufmann 1998; Rid 2012). Table 1 provides a snapshot of approaches to cyber security scholarship, as cited in Christou (2017).

Cyber Policies as Governance Indicator

Nye (2014) maintains that previous research has utilized the lens of regime theory as a method for elucidating complex international

Table 1 Approaches to Cyber Security Scholarship, as Cited in Christou (2017)

Research Approaches	Academic Literature
Traditional national strategic and managerial	Libicki (2007, 2009); Clarke and Knake (2010)
Historical	Carr (2009)
Terrorist-oriented	Wiemann (2006); Colarik (2006)
Governance (regulatory)	Mueller (2010); Brown and Marsden (2007)
Pragmatic, eclectic, comparative	Karatzogianni (2004, 2009); Eriksson and Giacomello (2010
Innovative mixed method	Deibert et al. (2011)
Securitized	Cavelty (2007, 2008); Bendrath, Eriksson, and Giacomello (2007)
Cyber power	Klimburg and Tiirmaa-Klaar (2011); Betz and Stevens (2011); Klimburg (2011); Nye (2010); Kramer, Starr, and Wentz (2009)

governance processes, thus providing a use case related to cyber governance. Other scholarship has employed similar approaches, utilizing the homeland security policy regime (May, Jochim, and Sapotichne 2011) and risk regimes (Quigley and Roy 2012) consistently with the goal of progressing policy regimes that concentrate policy making on a collective goal across diverse subsystems. Nye (2014, 19) concludes that "internet governance is the application by governments, the private sector and civil society of principles, norms, rules, procedures and programs that shape the evolution and use of the Internet." Other recent research has proposed that the citizenry has, in effect, become responsibilized—that cyber risk is individualized, thus contributing to the expansive spread and efficacy of cyber attacks (Hadjimatheou 2019; Renaud et al. 2018).

As noted by Harknett and Stever (2011, 455–456), the "cyber security problem does not fit conventional or traditional security categories based on individual security responsibilities, economic or corporate security issues, military security problems, as well as domestic versus international problems." The struggle, in determining the origins and impacts of a cyber attack, is "generally approached as a technical challenge for security professionals and politicians" (Schulzke 2018, 954). Schulzke (2018) argues that attributional challenges can affect a citizen's ability to cognize security challenges as well as evaluate government actions; this ambiguity often leaves citizens repeatedly missing the required information to ascertain dependably the attack perpetrators. Schulzke (2018, 954) presents that "attributional uncertainty immediately following cyber attacks encourages dependence on a narrow range of elite frames and the assignment of blame to familiar enemies."

Citizen Responsibilization

Citing the paradox in the current policy-making environment (de Bruijn and Janssen 2017), as well as other authors suggesting the murky pitfalls of attribution (Schulzke 2018), recent scholars have called for the framing of cyber security dialogue. Some have raised concerns about the apparent responsibilization of individuals for cyber security, comparing it with stances related to similar societal contagion-type risks such as disease and fire (Renaud et al. 2018).

Responsibilization may lead to the flawed conclusion that those who do not manage the risk, as they are expected to, *deserve* whatever outcomes that might ensue and that these unlucky individuals would then be stigmatized by their victimhood (Ekendahl, Mansson, and Karlsson 2018). The work of Quigley and Roy (2012, 83) most closely aligns with the precepts of responsibilization, employing an "anthropological understanding of risk in order to examine public sector action and capacity with respect to the multidimensional challenge of cyber security."

The aim of this article is to uncover the extent of cyber security responsibilization of individual citizens by six selected governments, as revealed by their own cyber security strategy policies.

Revealing Responsibilities and Intervention Stances

Governments' cyber security strategy policies are useful in revealing the mind-sets of governments in shaping cyber security provision and resilience. Evaluation of these policies can provide insights regarding what governments consider the roles of the citizen and organizations to be, as well as the intervention stance that governments adopt in considering the responsibilities of different stakeholders. The policy documents explain how governments say they will direct their efforts and, in some cases, allocate funding. Citing Doty (2015), de Bruijn and Janssen (2017) note that articulating a clear and concise message regarding cyber security policy is an onerous undertaking, one fraught with the task of conceptualizing future threats in a tactile manner without fostering a "fictionalization that might create a climate of fear" (Doty 2015, 342). The realm of cyber security is one of technical specialization and expertise that requires precise message framing, an approach for transmitting a complex civic issue with exactness and clarity. The crafting of cyber security policy often seeks lucidness in a division of labor regarding who bears different cyber responsibilities and the extent to which they are supported in acting on these. Yet thus far, there seems to be no clear idea of exactly what the responsibilities of each stakeholder are or how they ought to be allocated (de Bruijn and Janssen 2017).

Uncovering the underlying assumptions that drive the formulation of cyber security policies is essential because these assumptions about ability, confidence, and expertise to act reflect the cyber responsibilities that governments think entities ought to be embracing. Understanding these is important, because governments accept and allocate responsibility based on their conceptualization of the cyber security issue. If underlying self-efficacy assumptions are flawed, responsibilities might well be misaligned. Responsibilized parties may be unwilling, or unable, to accept and enact actions commensurate with implicitly assigned responsibilities.

Methodology

Our research uses a method extrapolated from an approach called *problematizing* (Bacchi 2009, 2012) to focus on the way responsibility is apportioned in the cyber security arena. Problematization is a rigorous and formalized way of revealing assumptions and critiquing solutions based on implicit problem conceptualizations. In our analysis, the extrapolation of Bacchi's problematization process to meet our analysis needs is referred to as a *responsibilization analysis*. This analysis poses six questions, analogous to Bacchi's problematization questions, to determine what the cyber responsibilities are and how they are currently allocated to citizens, organizations, and government—that is, what levels of intervention governments embrace in the cyber domain. We then consider these allocations and how the adopted intervention stances may be suboptimal. Our final question considers how the approach could be questioned and conceptualized differently. Figure 1 depicts the responsibilization analysis questions that were used during our analysis process and shows how these map to Bacchi's (2009, 2012) problematization questions.

Intervention Stances

To visualize the policy differences and similarities, we classified each responsibility in terms of intervention stance, similar to the scheme proposed by Assaf (2008). Responsibilities were categorized as follows:

Government (G_i) (maximal intervention): These are responsibilities that are fully embraced by the government, where no specific

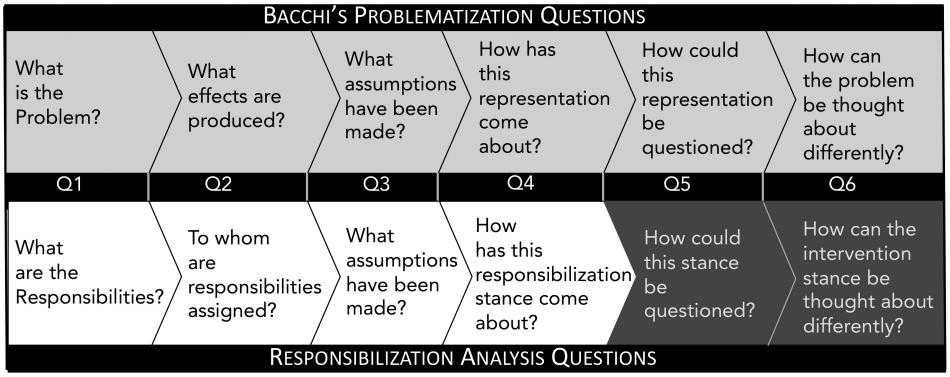

Figure 1 The Responsibilization Analysis Questions (Extrapolated from Bacchi's [2009] Problematization Questions)

stakeholder is mentioned. Examples are "manage and mitigate cyber threats," "engage internationally—laws, understanding, cooperation, info sharing," and "secure public sector organizations and infrastructures."

Monitor (M_i) (delegated intervention): Responsibilities include the words "ensure," "monitor," "hold . . . responsible," or "governance." In many cases, a specific stakeholder is mentioned—for example, "protect minors online." Finally, because all activities related to cyber criminals are delegated to law enforcement agencies, which report to and are monitored by the government, these, too, are classified as "monitor" responsibilities.

Service (S_i) (less intervention): Responsibilities resulting in some kind of outward-facing service, either explicitly or implicitly mentioned, are included in this category. Words indicating service-related responsibilities are "establish," "develop," "improve," "introduce," and "provide" are used with mention of a specific stakeholder. Examples are "improve skill sets of law enforcement" and "provide advice and set standards."

Voluntary (V_i) (no intervention): These responsibilities are neither monitored nor supported. Examples are "incentivize citizens to report cyber incidents" and "regular cyber testing of products by organizations."

Selecting Countries to Analyze

The first step in this evaluation focused on deciding which countries' strategy policies to analyze. We chose to examine countries that have, over the last few years, pursued a neoliberal agenda with respect to responsibility, given that citizen responsibilization is associated with government intervention stance. Government intervention in responsibilizing countries has shifted from maximum to minimum within the space of a few years.

To support cyber security intervention stance comparison, we thus chose to analyze the cyber security policies published by the Five Eyes countries—the United Kingdom (HM Government 2016), the United States (White House 2018), Canada (Public Safety Canada 2018), Australia (Australian Government 2016), and New Zealand (New Zealand Government 2015, 2018)—all of which are considered to be neoliberal in their government stance (Standford 2014; Weeks 2005), with an active responsibilization agenda (Kotz 2002). These countries constitute the world's most complete and comprehensive intelligence alliance (Tossini 2017), meaning that their cyber security stance can be expected to be mature. We chose to analyze the national cybersecurity policy of each country rather than policies formulated at the individual agency level because the cybersecurity policies offer a meaningful basis for comparison, while the countries' variation in size and composition would have made agency policy comparison infeasible. To facilitate comparison, we also analyzed the policy of China (USITO 2016), a country that, according to Chomsky (1999), is "the most interventionist and price-distorting government of all"—that is, it does not follow neoliberal dictates (Petersen 2018).

In focusing on responsibilization and aligned intervention stance, our analysis ought to reveal differences between the policies of China and the neoliberal Five Eyes countries. If governments *are* indeed responsibilizing their citizens with respect to cyber security, we should see this reality reflected in these countries' policy documents. Our analysis will also allow us to reveal how these countries propose to support their citizens in resisting cyber attacks and becoming cyber resilient.

The analysis was framed by investigations into similar documents carried out by Firmin and Gilson (2009) and Fitzgerald and Cunningham (2016)—that is, by formulating categories to use in classifying statements and then using those categories to identify the aligned cyber security responsibility. Statements in the countries' cyber security strategy policies were analyzed to reveal the stances of the governments with respect to managing the cyber risk.

Question 1: What Are the Responsibilities?

Each statement in policies was analyzed, to determine whether it:

G: mentioned the government *taking* responsibility for some action;

M: mentioned government *monitoring* the actions of some entity (citizen/industry) to ensure that they embrace their responsibility for cyber security, to ensure that the responsibility is accepted;

S: *assigned* a particular actionable responsibility for cyber security to a stakeholder, such as individual citizens or industry, or mentions some stakeholder (e.g., citizen/business) not accepting, or needing to embrace, a specific cyber security responsibility (less intervention); or.

V: mentioned that particular actions *ought* to be encouraged or carried out.

Generalized statements of responsibility, without attendant actions being expressly mentioned or implied, did not result in identification of a responsibility. For example, the statement from the Chinese translation, "The network affairs within the sovereignty of each country are the responsibility of the people of each country," does not meet the actionable requirement. Another statement from the same policy, "Encourage citizens to report cyber violations and bad information," aligns with the last category (V) and thus is counted as a responsibility.

Our analysis resulted in 86 "responsibilities" across all policies (see the appendix S1 in the Supporting Information online). We merged those that were semantically similar, leaving a final set of 68 distinct responsibilities. The next step was to identify those that applied specifically to citizens, as opposed to those embraced by governments themselves or assigned to organizations, educational authorities, or researchers.

Some responsibilities are mentioned by all the policies: secure government systems (G9), invest in security (G1, M4), keep up with emergent threats (G5), increase the number of people skilled in cyber security (S1), ensure that organizations adopt secure behaviors (M2) and improve security awareness (S2, S6). This confirms responsibilities mentioned by Norris et al. (2017, 2018, 2019). Yet only a handful of statements specifically refer to citizens, the main beneficiaries being organizations and governments (S1, S5, S6, S7, S12).

Question 2: To Whom Are Responsibilities Assigned?

Evaluation of the policies from the Five Eyes countries and China revealed that governments mention many responsibilities, including dealing with cyber criminals (M1), protecting government infrastructures (G9), and strengthening international collaboration with other countries in enhancing global cybercrime management (G7). While these actions are crucial, citizens and organizations are as vulnerable to attack as government systems—perhaps even more so.

The purpose of this analysis was to reveal what governments believe the responsibilities of individual citizens to be and to identify the direct support that governments provide to their citizens. In theory, government support can range from relatively low intervention, such as the provision of advice, or providing their citizens with the tools and assistance to protect themselves in the cyber domain (Assaf 2008). Even if governments do not "own" specific responsibilities, they could exercise a slightly reduced measure of intervention by monitoring responsibility-related behaviors. This possibility is mentioned when it comes to organizations (M2, M4), but monitoring citizen actions in the cyber realm is only mentioned in the Chinese policy (M5, M6, M7, M8). The responsibilities mentioned by other countries, related specifically to citizens, include public awareness campaigns (S14), provision of advice (S2), providing tools (S19), and encouraging reporting of crimes (V3). This is a manifestation of a typical responsibilization stance. Indeed, the Australian policy includes this statement: "We are all responsible for our own activities in cyberspace, including being aware of the risks and how to protect ourselves and those who we are connected to" (Australian Government 2016, 23).

Figure 2 shows the number of responsibilities, for each country, in each of these intervention categories. The anticipated differences between China and the other countries is indeed apparent.[4]

Figure 3 shows the intervention stance applied to citizens on the government intervention scale.

Question 3: What Assumptions Have Been Made?

Based on the analysis, and focusing on what the policies say about citizens, most Five Eyes governments offer advice and expect citizens to take care of themselves when it comes to resisting cyber attacks and to report attacks (voluntarily) when these occur. The core assumptions of this responsibilization approach are that people will (1) gain access to this advice, (2) understand the need to heed it and trust it, (3) act on the advice and/or be able to utilize the provided tools, and (4) report attacks. Whether or not evidence exists for the viability of these assumptions warrants further debate.

Assumption 1: The problem with cyber advice is that there is no obvious route by which such advice can be delivered, reliably, to every citizen (Okuku, Renaud, and Valeriano 2015). Certainly, some people may seek advice, but many turn to Google (Renaud

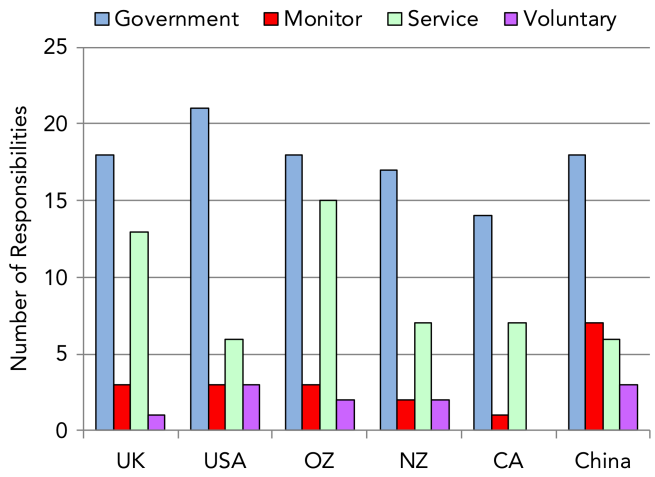

Figure 2 Countries' Cumulative Responsibilities, Ranging from Maximum Intervention (Government) to Minimal Intervention (Voluntary)

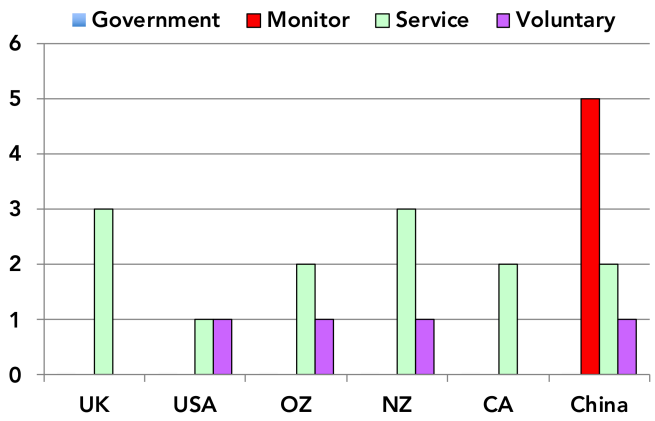

Figure 3 Governments' Intervention Stances for Citizen Cyber Threat Management

and Weir 2016) or rely on a family friend (Poole et al. 2009). As a consequence, they may not receive accurate advice or be so bewildered by the sheer amount of advice that they give up altogether (Bawden and Robinson 2009). In summary, there is no guarantee that any individual will become aware of high value cyber security good practice advice.

Assumption 2: Risk perceptions do indeed predict adoption of precautionary cyber security behaviors (van Schaik et al. 2018). However, facts and knowledge, on their own, do not reliably lead to accurate risk perceptions (Cross 1998; Pidgeon et al. 1992) because risk perception is both objective (fact based) and subjective (socially constructed and emotional) (Hansson 2010). While facts might well make an impact, they could easily be overridden by subjective aspects, which could lead to the recipient rejecting the import of the facts.

Assumption 3: Even if citizens are exposed to the requisite cyber security knowledge and decide to take notice of it, it cannot be taken for granted that they will act on that knowledge (Campbell 2012; de Neufville 1987; Geller, Erickson, and Buttram 1983; Holcomb et al. 2009). People rely on heuristics, feelings, biases, and emotional reasoning when acting on knowledge (Gigerenzer and Gaissmaier 2011). Information may guide decisions to act, but this link is by no means certain or reliable. There is evidence for this tendency in cyber security (Bada and Sasse 2014).

Assumption 4: The final assumption is that people will report attacks, but the evidence suggests that this is not happening at present (Mills 2017). Moreover, this also assumes that people will know they have been attacked when, as Norris et al. (2019) point out, even local governments do not always know that this has happened. Citizens cannot be expected to have a great deal of expertise and it is likely that they sometimes will not even know that their device has been compromised.

Given the fact that the four underlying assumptions stated at the beginning of this section are unsupported, the responsibilization of citizens, when it comes to the cyber security of their information and devices, seems unrealistic.

Question 4: How Has This Responsibilization Stance Come About?

One explanation for what we found is the natural shift in neoliberal countries in the twenty-first century. In these countries, it has become implicitly accepted that individuals should be responsible for their own choices and the consequences of those choices. This responsibilization renders citizens individually responsible for a task that might previously have been the responsibility of some government agency (Wakefield and Fleming 2008). Over recent decades, responsibility has indeed been shifted from many governments to individuals in a variety of areas (Comack and Peter 2005). Citizens are advised on what actions to take, made responsible for the actions they choose to take, and then must accept the outcomes, good or bad. The message, and government agenda, is that "whether it is the labor market, retirement, health care or crime, individuals are activated and encouraged to take care of themselves" (Biebricher 2011, 472). There is much evidence that many Western governments responsibilize their citizens, holding them responsible for becoming the victims of crime (Grubb and Turner 2012), their own unemployment (Biebricher 2011; Harding 1985), their safety (Gray 2009), community crime (Skinns 2003), and even border control (Koskela 2011). Avigur-Eshel (2018) points out that individuals have even been blamed for social problems such as inequality and the instability of the financial system (citing Finlayson 2009; OECD 2009). Cyber security responsibilization extends this approach to a new domain.

Another possible explanation is that cyber security, with its cyber "criminals" and mention of "attacks" and "securing" of devices, creates parallels in the minds of policy makers with security in the physical realm. This duality might have led governments to apply the same solutions to the virtual world as those that have become entrenched in the physical world. Householders are expected to secure their personal dwellings and properties and it might be assumed that they can do the same when it comes to cyber security.

A third explanation is alluded to in a statement by General Michael Hayden, former director of the Central Intelligence Agency: "Rarely has something been so important and so talked about with less clarity and less apparent understanding [than cyber security]. . . . I have sat in very small group meetings in Washington. . . unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of any decision we might make" (Hayden 2011, 3). The argument is that the newness of this domain prevents clear-sighted and effective decision-making in terms of how best to manage the threats and has led to unrealistic expectations of citizen capabilities.

A complicated phenomenon, such as responsibilization, is unlikely to have a single causative, and a full exploration of causes, while important and worthy of investigation, is off topic for this article.

Questions 5 and 6: How Could the Intervention Stance Be Questioned/Thought about Differently?

The fact that governments are responsibilizing their citizens when it comes to cyber security seems to be just another instance of governmental responsibilization of citizens, reminiscent of using what has worked before, without contemplating that the context might render the usual approach inappropriate (Bednar and Page 2018). Responsibilization has not seen unqualified success in other areas (Avigur-Eshel 2018; Phoenix and Kelly 2013; Rossiter 2012; Soneryd and Uggla 2015; Stol, Schermer, and Asscher 2016), notably in those domains where building capability is rather more challenging than anticipated (e.g., health, finance, and drug abuse). Renaud et al. (2018) suggest that responsibilizing cyber security is ill advised and that more should be done to support citizens and organizations in resisting cyber attacks. They argue that cyber threats are currently managed by governments as if they are a solo risk, whereas they ought to be managed similar to the way other contagious and calamitous risks are managed, due to the epidemiology of cyber attacks and the expertise required to mitigate them.

Analysis of the cyber security strategy policies of the six countries included in this study revealed that the Five Eyes governments

relegate the responsibility for protection from cyber attacks to their individual citizens. Government efforts are often concentrated on the protection of their own information infrastructure and assets (G9), cybercrime prevention and deterrence (M1), managing and mitigating threats (G5), and strengthening international cooperation (G7). However, they rarely focus on directly supporting citizens to combat identity theft or coping with the consequences of ransomware, fraud, and other cybercrimes. Changes in government strategies are needed to more equitably and realistically allocate responsibilities and to provide more substantial support to individuals and entities in carrying out their cyber security related activities. In other domains, such as the treatment of sex offenders (Adam 2012), the Belgian government, for one, has now de-responsibilized this activity. It seems time for us to reevaluate the cyber-related responsibilization of citizens too.

As global populations increasingly connect to the internet, the implementation and ongoing management of governance structures and policy is garnering attention and deliberation from citizens, much like health and education reforms. Governments must embrace their roles and confront the myriad of challenges that come from a shared responsibility to diminish cyber security risks for everyone.

The Five Eyes countries apply a responsibilization agenda, while China exercises a measure of control by monitoring citizen behaviors and expecting good online citizenship. It is unlikely that citizens of the Five Eyes countries would accept such monitoring of their devices and online activities, given the cultural differences between the countries (Kharlamov and Pogrebna 2019). Moreover, Chang, Zhong, and Grabosky (2018) suggest that it is essential for citizens to be partners in the fight against cyber crime. The question is, "how do we achieve this?" One approach worth considering, which does not require ratcheting up intervention and monitoring, is suggested by Ahrens and Rudolph (2006, 207), which aims to "create capabilities of both public and private stakeholders." Their approach is built on four governance dimensions: predictability, transparency, participation, and accountability. They argue that "governance structure is effective and market-enhancing if it ensures that government policies are properly implemented, that private businesses can thrive within a given legal and regulatory framework and that the adaptive efficiency of both the polity and the economy is enhanced" (Ahrens and Rudolph 2006, 212). Ahrens and Rudolph explain that *accountability* constitutes an agreement on roles and responsibilities of organizations and individuals. It also entails reporting on the actions taken. This makes it possible for stakeholders to ensure that their views and needs have been considered and that performance is adequate. *Participation* requires all stakeholders to be involved in the policy-making process so that the services they deem essential are provided. *Transparency* goes hand in hand with accountability, and can encourage participation of stakeholders. *Predictability* requires actions to be formulated in a rule-based fashion, binding public officials and private actors. Such rules make it possible for community expectations to be established, understood, accepted, and managed.

The way governments are currently supporting individuals does not always satisfy these principles. For example, some governments have been criticized by privacy advocates over recent years for a lack of transparency and accountability for their actions in cyberspace (Grabianowski 2007; Landau 2020; Liberty 2018). Moreover, as we report, there is no widely adopted set of roles and responsibilities in this space (de Bruijn and Janssen 2017), which the predictability principle requires. A perusal of the policies also suggests that while industry and academia have fed into the formulation of the policies, the voices of individual citizens have been given less prominence, as evidenced by the paltry support they receive. A new dispensation, based on Ahrens and Rudolph's principles from disaster management, is worth considering.

Challenges in Implementing Policies

Despite the ubiquity of devices that connect individuals not only to each other but across society at large, cyber security remains an underdeveloped topic of research. This applies from the perspective not only of public administration but also of the creation, implementation, and ongoing management of governance structures and policy. The swift adoption of Internet-of-Things devices, connected to, and communicating across, the internet, is set to exceed the impact of the internet itself (Shrouf and Miragliotta 2015), only raising the stakes for governments, organizations, and individuals in what has become the ever-pressing task of staying vigilant and secure. Moreover, vying for and obtaining the resources to ensure that information and communication systems remain secure has remained a task not to be taken for granted. This is evidenced in the (Deloitte-NASCIO 2014) Cyber security study, citing a budget-strategy disconnect apparent in many state governments that leads to inadequate allocation of funds to cyber budgets. That finding readily expresses the challenge faced in articulating the seriousness of the cyber threat as it exists today. In fact, communicating the criticality of risks posed by cyber threats (de Bruijn and Janssen 2017) is likely to be as demanding as uncovering and mitigating the actual security problem.

It is imperative that elected officials and policy makers come to understand the potential economic and societal impact of cyber security breaches. In addition to the impact on the individual citizen—often left to their own devices to protect themselves from cybercrime—the "issue of security is not limited to the executive power, but is also relevant to political parties, energy infrastructure providers, water boards, road management, ministries, administrative organizations, NGOs and even sporting organizations" (de Bruijn and Janssen 2017, 1). Cyber security breach data and subsequent analyses suggest that financial outlays for security breach remediation are increasing. According to the Global Cost of Data Breach Study (Ponemon 2018), the cost, on average, to remediate a data breach increased 6.4 percent over the previous year to $3.86 million, while the average cost for each compromised record containing sensitive and confidential information also increased by 4.8 percent year-over-year to $148. In addition, consider a report from the Identity Theft Resource Center (CyberScout 2016), which notes that, beyond the rising costs for remediation, breaches are occurring at a markedly higher rate, with estimates of year-on-year increases of 40 percent, with nearly a third being public sector entities.

Conclusion and Future Work

This article commenced by asking what intervention stances governments adopt in supporting individual citizens managing their personal cyber risk. Analysis of the cyber security strategy policies

revealed low levels of Five Eyes' government intervention, in stark contrast with the greater levels of support offered to organizations and funding research endeavors. Five Eyes citizens are effectively left to secure their own devices and repel the efforts of myriad cyber criminals across the globe, armed only with accurate advice that they may not find and not be able to follow, even if they do obtain and understand it. There is more monitoring of citizens in China, but the level of support is not markedly different from that in the Five Eyes countries.

Evidence exists that a responsibilization approach is not particularly effective in this domain: individuals are being hacked and suffering negative consequences, with no signs that attacks are abating. Most governments focus on catching and prosecuting cyber criminals. While this strategy works well in the physical world for other types of crimes, it must be noted that the cyber security world does not mirror the physical world. Nye (2011, 21) points out that "actors are diverse, sometimes anonymous, physical distance is immaterial, and offense is often cheap." Cyber criminals across the globe can, and do, target people without requiring physical proximity. If one person's device is compromised by a cyber criminal, the exploit could spread to all their connections. Physical crime does not necessarily exhibit this epidemiological characteristic. Finally, individuals are very knowledgeable about securing their physical belongings and themselves, because mankind has been doing this for thousands of years. Yet relatively few citizens have mastered the skills required to secure their devices and online accounts. Thus, governments need to do more to protect their citizens from cyber attacks. New Zealand's policy (New Zealand Government 2018) mentions providing cyber-related tools to their citizens, a welcome step in this direction.

Development of a feasible plan for de-responsibilizing citizens is beyond the scope of this article, but offers several avenues for future research. Two endeavors are worth mentioning. The first, by the Israeli government, is the establishment of a Cyber-Hotline for people to report being hacked and to receive help with solutions (Williams 2019). The second is what the British call "Cyberhood Watch," which suggests training people to help others in their communities with their cyber problems (Carpani 2019). Future research efforts should also explore the degree to which governments have incorporated various factors and models into their cyber security policy formation processes. Specifically, are considerations of shared costs and benefits—public goods or shared public costs—considered when citizens are asked to take their own responsibility for cyber security management? More generally, how and why do governments choose their respective policy stances around individual citizens' cyber security?

We believe that governments who have not yet envisaged these kinds of solutions should reconsider whether their current stance, and the effective cyber responsibilization of their citizens, is indeed appropriate (Renaud et al. 2018). Our investigation, in revealing the responsibilization stances, should impact future research in public administration.

Notes

1. Christou (2017) notes that a significant portion of the work highlights efforts in the United States, fewer do so in the European Union, but with no agreed upon inclusive theoretical framework. Recognizing the fluidity of the cyber world, Christou acknowledges cyber power as a predominant driver for contextualizing approaches to cyber security and offers a brief, but thorough, summary of literature focused on a subsequent handful of approaches utilized to bring clarity to cyber governance and policy development.
2. International Telecommunication Union, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cyber security-index.aspx.
3. See National Cyber Security Index 2018 at https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf and http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (accessed April 5, 2020).
4. This analysis focused on the national cybersecurity policy documents issued at the highest level of government. We acknowledge that a different level of intervention could be detailed within other agency level documents, which is likely to be the case in the United States. While a review of agency level documents is beyond the scope of this study, this type of analysis presents a fruitful avenue for future research.

References

ABC7 Chicago. 2017. Wired Away: Couple Loses Life Savings during Home Purchase. November 13. https://abc7chicago.com/realestate/wired-away-couple-loses-life-savings-during-home-purchase/2630496/ [accessed May 7, 2020].

Adam, Christophe. 2012. Responsibilization and De-Responsibilization in the Treatment of Sex Offenders in Belgium. *Déviance et Société* 36(3): 263–76. https://doi.org/10.3917/ds.363.0263.

Ahrens, Joachim, and Patrick M. Rudolph. 2006. The Importance of Governance in Risk Reduction and Disaster Management. *Journal of Contingencies and Crisis Management* 14(4): 207–20. https://doi.org/10.1111/j.1468-5973.2006.00497.x.

AlDairi, Anwaar, and Lo'ai Tawalbeh. 2017. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science* 109: 1086–91. https://doi.org/10.1016/j.procs.2017.05.391.

Andreasson, Kim J., ed. 2011. *Cybersecurity: Public Sector Threats and Responses*. Boca Raton, FL: CRC Press.

Assaf, Dan. 2008. Models of Critical Information Infrastructure Protection. *International Journal of Critical Infrastructure Protection* 1: 6–14. https://doi.org/10.1016/j.ijcip.2008.08.004.

Australian Government. 2016. Australia's Cyber Security Strategy. https://cybersecuritystrategy.homeaffairs.gov.au/ [accessed May 7, 2020].

Avigur-Eshel, Amit. 2018. Depoliticization and Responsibilization: The Case of Financial Education in Israel. *Competition & Change* 22(5): 509–28. https://doi.org/10.1177/1024529418798115.

Bacchi, Carol. 2009. *Analysing Policy: What's the Problem Represented to Be?* Pearson Australia: Frenchs Forest, Australia.

———. 2012. Why Study Problematizations? Making Politics Visible. *Open Journal of Political Science* 2(1): 1–8. https://doi.org/10.4236/ojps.2012.21001.

Bada, Maria, and M. Angela Sasse. 2014. *Cyber Security Awareness Campaigns: Why Do They Fail to Change Behavior?* Global Cyber Security Capacity Centre, University of Oxford. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-awareness-campaigns-why-do-they-fail-change-behaviour [accessed May 7, 2020].

Bawden, David, and Lyn Robinson. 2009. The Dark Side of Information: Overload, Anxiety and Other Paradoxes and Pathologies. *Journal of Information Science* 35(2): 180–91. https://doi.org/10.1177/0165551508095781.

Bednar, Jenna, and Scott E. Page. 2018. When Order Affects Performance: Culture, Behavioral Spillovers, and Institutional Path Dependence. *American Political Science Review* 112(1): 82–98. https://doi.org/10.1017/S0003055417000466.

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello. 2007. From "Cyberterrorism" to "Cyberwar," Back and Forth. In *International Relations and*

Security in the Digital Age, edited by Johan Eriksson and Giampiero Giacomello, 57–82. Abingdon: Routledge. https://doi.org/10.4324/9780203964736.

Betz, David J., and Tim Stevens. 2011. *Cyberspace and the State: Towards a Strategy for Cyber-Power*. Oxford: Routledge.

Biebricher, T. 2011. (Ir-) Responsibilization, genetics and neuroscience. *European Journal of Social Theory* 14(4): 469–88.

Bretschneider, Stuart. 1990. Management Information Systems in Public and Private Organizations: An Empirical Test. *Public Administration Review* 50(5): 536–45. https://doi.org/10.2307/976784.

Brown, Ian, and Chris Marsden. 2007. Co-Regulating Internet Security: the London Action Plan. http://www.academia.edu/686684/Coregulating_Internet_security_the_London_Action_Plan [accessed May 7, 2020].

Campbell, Heather. 2012. Planning to Change the World: Between Knowledge and Action Lies Synthesis. *Journal of Planning Education and Research* 32(2): 135–46. https://doi.org/10.1177/0739456X11436347.

Carpani, Jessica. 2019. *Cyberhood Watch: Curtain Twitchers Become IT Helpdesk for Neighbours*. *Telegraph* (London), November 9. https://www.telegraph.co.uk/news/2019/11/09/cyberhood-watch-curtain-twitchers-become-helpdesk-neighbours/ [accessed May 7, 2020].

Carr, Madeline. 2016. Public–Private Partnerships in National Cyber-Security Strategies. *International Affairs* 92(1): 43–62. https://doi.org/10.1111/1468-2346.12504.

Caruson, Kiki, Susan A. MacManus, and Brian McPhee. 2012. Cyber Security at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs* 35(4): 451–70. https://doi.org/10.1111/j.1467-9906.2012.00640.x.

Caudle, Sharon L. 1990. Managing Information Resources in State Government. *Public Administration Review* 50(5): 515–24. https://doi.org/10.2307/976782.

Cavelty, Myriam Dunn. 2007. Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology and Politics* 4(1): 19–35. https://doi.org/10.1300/J516v04n01_03.

———. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. New York: Routledge.

Chang, Lennon Y.C., Lena Y. Zhong, and Peter N. Grabosky. 2018. Citizen Co-production of Cyber Security: Self-Help, Vigilantes, and Cybercrime. *Regulation & Governance* 12(1): 101–14. https://doi.org/10.1111/rego.12125.

Christou, George. 2017. *The EU's Approach to Cyber Security*. Online Paper Series, University of Essex. http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf [accessed May 7, 2020].

Cho, Chung-Lae, and Deil S. Wright. 2004. The Devolution Revolution in Intergovernmental Relations in the 1990s: Changes in Cooperative and Coercive State-National Relations as Perceived by State Administrators. *Journal of Public Administration Research and Theory* 14(4): 447–68. https://doi.org/10.1093/jopart/muh031.

Chomsky, Noam. 1999. *Profit over People: Neoliberalism and Global Order*. New York: Seven Stories Press.

Christensen, Kristoffer K., and Karen L. Petersen. 2017. Public–Private Partnerships on Cyber Security: A Practice of Loyalty. *International Affairs* 93(6): 1435–52. https://doi.org/10.1093/ia/iix189.

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: HarperCollins.

Colarik, Andrew M. 2006. *Cyber Terrorism: Political and Economic Implications*. London: IGI Publishing.

Comack, Elizabeth, and Tracey Peter. 2005. How the Criminal Justice System Responds to Sexual Assault Survivors: The Slippage between "Responsibilization" and "Blaming the Victim". *Canadian Journal of Women and the Law* 17(2): 283–309. https://www.muse.jhu.edu/article/213365.

Cordes, Joseph J. 2010. An Overview of the Economics of Cybersecurity and Cybersecurity. Report GW-CSPRI-2011-6, George Washington University, Cyber Security Policy and Research Institute, June 1. http://infosecon.net/workshop/downloads/2011/pdf/An_Overview_of_the_Economics_of_Cybersecurity_and_Cybersecurity_Policy.pdf [accessed May 7, 2020].

Coursey, David, and Donald F. Norris. 2008. Models of E-Government: Are They Correct? An Empirical Assessment. *Public Administration Review* 68(3): 523–36. https://doi.org/10.1111/j.1540-6210.2008.00888.x.

Cross, Frank B. 1998. Facts and Values in Risk Assessment. *Reliability Engineering & System Safety* 59(1): 27–40. https://doi.org/10.1016/S0951-8320(97)00116-6.

CyberScout. 2016. Identity Theft Resource Centers Data Breach Reports: 2016 End of Year Report. https://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf. [accessed May 7, 2020].

de Bruijn, Hans, and Marijn Janssen. 2017. Building Cybersecurity Awareness: The Need for Evidenced-Based Framing Strategies. *Government Information Quarterly* 34(1): 1–7. https://doi.org/10.1016/j.giq.2017.02.007.

de Neufville, Judith Innes. 1987. Knowledge and Action: Making the Link. *Journal of Planning Education and Research* 6(2): 86–92. https://doi.org/10.1177/0739456X8700600203.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2011. *Access Contested: Security, Identity and Resistance in Asian Cyberspace*. Cambridge, MA: MIT Press.

Desouza, Kevin C., and Akshay Bhagwatwar. 2012. Leveraging Technologies in Public Agencies: The Case of the U.S. Census Bureau and the 2010 Census. *Public Administration Review* 72(4): 605–14. https://doi.org/10.1111/j.1540-6210.2012.02592.x.

Doty, Phillip. 2015. U.S. Homeland Security and Risk Assessment. *Government Information Quarterly* 32(3): 342–52. https://doi.org/10.1016/j.giq.2015.04.008.

Ekendahl, Mats, Josefin Mansson, and Patrik Karlsson. 2018. Risk and Responsibilization: Resistance and Compliance in Swedish Treatment for Youth Cannabis Use. *Drugs: Education, Prevention and Policy* 27(1): 60–8. https://doi.org/10.1080/09687637.2018.1544224.

Elazar, Daniel J. 1990. Opening the Third Century of American Federalism: Issues and Prospects. *Annals of the American Academy of Political and Social Science* 509: 11–21. https://doi.org/10.1177/0002716290509001002.

Eriksson, Johan, and Giampiero Giacomello, eds. 2010. *International Relations and Security in the Digital Age*. New York: Routledge.

Farrand, Benjamin, and Helena Carrapico. 2018. Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism. In *Security Privatization*, edited by Oldrich Bures and Helena Carrapico, 197–217. Geneva: Springer International. https://doi.org/10.1007/978-3-319-63010-6_9.

Finlayson, Alan. 2009. Financialisation, Financial Literacy and Asset-Based Welfare. *British Journal of Politics and International Relations* 11(3): 400–21. https://doi.org/10.1111/j.1467-856X.2009.00378.x.

Firmin, Michael W., and Krista M. Gilson. 2009. Mission Statement Analysis of CCCU Member Institutions. *Christian Higher Education* 9(1): 60–70. https://doi.org/10.1080/15363750903181922.

Fitzgerald, Clara, and James A. Cunningham. 2016. Inside the University Technology Transfer Office: Mission Statement Analysis. *Journal of Technology Transfer* 41(5): 1235–46. https://doi.org/10.1007/s10961-015-9419-6.

Gartzke, Erik. 2013. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security* 38(2): 41–73. https://doi.org/10.1162/ISEC_a_00136.

Gatlan, Sergiu. 2020. Coronavirus Phishing Attacks Are Actively Targeting the US. Bleeping Computer, February 1. https://www.bleepingcomputer.com/news/security/coronavirus-phishing-attacks-are-actively-targeting-the-us/ [accessed May 7, 2020].

Geller, E. Scott, Jeff B. Erickson, and Brenda A. Buttram. 1983. Attempts to Promote Residential Water Conservation with Educational, Behavioral and Engineering Strategies. *Population and Environment* 6(2): 96–112. https://doi.org/10.1007/BF01362290.

Gigerenzer, Gerd, and Wolfgang Gaissmaier. 2011. Heuristic Decision Making. *Annual Review of Psychology* 62: 451–82. https://doi.org/10.1146/annurev-psych-120709-145346.

Glaser, Charles L., and Chaim Kaufmann. 1998. What Is the Offense-Defense Balance and Can We Measure it? *International Security* 22(4): 44–82. https://doi.org/10.1162/isec.22.4.44.

Goodyear, Marilu, Holly T. Goerdel, Shannon Portillo, and Linda Williams. 2010. Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers. IBM Center for the Business of Government. http://www.businessofgovernment.org/report/cybersecurity-management-states-emerging-role-chief-information-security-officers [accessed May 7, 2020].

Grabianowski, Ed. 2007. How the Patriot Act Works. howstuffworks.com, July 6. https://people.howstuffworks.com/patriot-act.htm [accessed May 7, 2020].

Gray, Garry C. 2009. The Responsibilization Strategy of Health and Safety Neo-liberalism and the Reconfiguration of Individual Responsibility for Risk. *British Journal of Criminology* 49(3): 326–42. https://doi.org/10.1093/bjc/azp004.

Grubb, Amy, and Emily Turner. 2012. Attribution of Blame in Rape Cases: A Review of the Impact of Rape Myth Acceptance, Gender Role Conformity and Substance Use on Victim Blaming. *Aggression and Violent Behavior* 17(5): 443–52. https://doi.org/10.1016/j.avb.2012.06.002.

Hadjimatheou, Katerina. 2019. Citizen-Led Digital Policing and Democratic Norms: The Case of Self-Styled Paedophile Hunters. *Criminology & Criminal Justice*. Published online October 16. https://doi.org/10.1177/1748895819880956.

Hansson, Sven Ove. 2010. Risk: objective or subjective, facts or values. *Journal of risk research* 13(2): 231–38.

Harding, Ann. 1985. Unemployment Policy: A Case Study in Agenda Management. *Australian Journal of Public Administration* 44(3): 224–46. https://doi.org/10.1111/j.1467-8500.1985.tb02443.x.

Harknett, Richard J., and James A. Stever. 2009. The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management* 6(1): 1–13. https://doi.org/10.2202/1547-7355.1649.

———. 2011. The New Policy World of Cyber Security. *Public Administration Review* 71(3): 455–60. https://doi.org/10.1111/j.1540-6210.2011.02366.x.

Hathaway, Melissa. 2014. Connected Choices: How the Internet Is Challenging Sovereign Decisions. *American Foreign Policy Interests* 36(5): 300–13. https://doi.org/10.1080/10803920.2014.969178.

Hathaway, Melissa, and John Stewart. 2014. Taking Control of our Cyber Future. *Georgetown Journal of International Affairs* 2014: 55–68. https://www.jstor.org/stable/43773649.

Hayden, Michael V. 2011. The Future of Things "Cyber.". *Strategic Studies Quarterly* 5(1): 3–7. https://doi.org/10.1201/b15253.

Her Majesty's (HM) Government. 2016. National Cyber Security Strategy 2016–2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 [accessed May 7, 2020].

Ho, Alfred Tat-Kei. 2002. Reinventing Local Governments and the E-Government Initiative. *Public Administration Review* 62(4): 434–45. https://doi.org/10.1111/0033-3352.00197.

Holcomb, Tim R., R. Duane Ireland, Michael Holmes Jr, and Michael A. Hitt. 2009. Architecture of Entrepreneurial Learning: Exploring the Link among Heuristics, Knowledge, and Action. *Entrepreneurship Theory and Practice* 33(1): 167–92. https://doi.org/10.1111/j.1540-6520.2008.00285.x.

Hughes, Kate. 2020. Coronavirus Fraud Warnings as Britons Lose £800,000 since Outbreak Arrived. *Independent* (London), March 17. https://www.independent.co.uk/money/spend-save/fraud-scams-coronavirus-phishing-tricks-malware-refund-push-payment-a9405846.html [accessed May 7, 2020].

Irwin, Luke. 2020. List of Data Breaches and Cyber Attacks in February 2020–623 million Records Breached. *IT Governance* (blog), March 2. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2020-623-million-records-breached [accessed May 7, 2020].

Karatzogianni, Athina. 2004. The Politics of "Cyberconflict.". *Politics* 24(1): 46–55. https://doi.org/10.1111/j.1467-9256.2004.00204.x.

———. 2009. How Small Are Small Numbers in Cyberspace? Small, Virtual Wannabe "States," Minorities and Their Cyberconflicts. In *Cyberconflict and Global Politics*, edited by A. Karatzogianni, 128–45. London: Routledge. https://doi.org/10.4324/9780203890769.

Kello, Lucas. 2013. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security* 38(2): 7–40. https://doi.org/10.1162/ISEC_a_00138.

Kharlamov, Alexander, and Ganna Pogrebna. 2019. Using Human Values-Based Approach to Understand Cross-Cultural Commitment toward Regulation and Governance of Cybersecurity. *Regulation & Governance*. Published online October 4. https://doi.org/10.1111/rego.12281.

Kincaid, John, and Richard L. Cole. 2002. Issues of Federalism in Response to Terrorism. Special issue. *Public Administration Review* 62: 181–92. https://doi.org/10.1111/1540-6210.62.s1.28.

Klimburg, Alexander. 2011. Ruling the Domain: (Self) Regulation and the Security of the Internet. Austrian Institute for International Affairs. http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Ruling_the_Domain_Klimburg.pdf [accessed January 2, 2018].

Klimburg, Alexander, and Heli Tiirmaa-Klaar. 2011. *Cyber War and Cyber Security: Challenges Faced by the EU and its Member States*. Directorate-General for External Policies, Policy Department, European Parliament. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO-SEDE_ET(2011)433828 [accessed May 7, 2020].

Koskela, Hille. 2011. "Don't Mess with Texas!" Texas Virtual Border Watch Program and the (Botched) Politics of Responsibilization. *Crime, Media, Culture* 7(1): 49–65. https://doi.org/10.1177/1741659010369957.

Kotz, David M. 2002. Globalization and Neoliberalism. *Rethinking Marxism* 14(2): 64–79. https://doi.org/10.1080/089356902101242189.

Kraemer, Kenneth L., and William H. Dutton. 1978. Management Utilization of Computers in American Local Government. *Communications of the ACM* 21(3): 206–18. https://doi.org/10.1145/359361.359364.

Kramer, Franklin, Stuart H. Starr, and Larry Wentz, eds. 2009. *Cyber Power and National Security*. Washington, DC: National Defense University Press.

Kubiak, Paloma. 2020. Victims Lose £1m to Coronavirus Scams. YourMoney.com, March 20. https://www.yourmoney.com/household-bills/victims-lose-1m-to-coronavirus-scams/ [accessed May 7, 2020].

Kuehn, Andreas. 2014. Extending Cyber Security, Securing Private Internet Infrastructure: The US Einstein Program and its Implications for Internet Governance. In *The Evolution of Global Internet Governance*, edited by Roxana Radu, Jean-Marie Chenou, and Rolf H. Weber, 157–67. Berlin, Germany: Springer. https://doi.org/10.1007/978-3-642-45299-4_9.

Kuerbis, Brenden, and Farzaneh Badiei. 2017. Mapping the Cyber Security Institutional Landscape. *Digital Policy, Regulation and Governance* 19(6): 466–92. https://doi.org/10.1108/DPRG-05-2017-0024.

Landau, Susan. 2020. Location Surveillance to Counter COVID-19: Efficacy Is What Matters. *Lawfare* (blog), March 25. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters [accessed May 7, 2020].

Lee, Chung-pin, Kaiju Chang, and Frances S. Berry. 2011. Testing the Development and Diffusion of e-Government and e-Democracy: A Global Perspective. *Public Administration Review* 71(3): 444–54. https://doi.org/10.1111/j.1540-6210.2011.02228.x.

Liberty. 2018. The Snooper's Charter. https://www.libertyhumanrights.org.uk/human-rights/privacy/snoopers-charter [accessed May 7, 2020].

Libicki, Martin C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.

——— 2009. *Cyber Deterrence and Cyber War. Prepared for the United States air Force*. Santa Monica, CA: RAND Corporation.

Lkhagvasuren, Galbaatar. 2017. Cyber Security Cooperation of Countries: Impact of Draft International Code of Conduct for Information Security. In *Proceedings of*

the 10th International Conference on Theory and Practice of Electronic Governance, edited by Rehema Baguma, Rahul De', and Tomasz Janowski, 564–5. https://doi.org/10.1145/3047273.3047317.

Luiijf, Eric, Kim Besseling, and Patrick de Graaf. 2013. Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructures* 9(1–2): 3–31. https://doi.org/10.1504/IJCIS.2013.051608.

May, Peter J., E. Jochim Ashley, and Joshua Sapotichne. 2011. Constructing Homeland Security: An Anemic Policy Regime. *Policy Studies Journal* 39(2): 285–307. https://doi.org/10.1111/j.1541-0072.2011.00408.x.

Mills, James. 2017. Too Many People Are Afraid to Report Cybercrime—But It Can Be Stopped. *Telegraph* (London), November 10. https://www.telegraph.co.uk/news/2017/11/10/many-people-afraid-report-cybercrime-can-stopped/ [accessed May 7, 2020].

Moon, M. Jae. 2002. The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public Administration Review* 62(4): 424–34. https://doi.org/10.1111/0033-3352.00196.

Mueller, Milton. 2010. *Networks and States: The Global Politics of the Internet*. Cambridge, MA: MIT Press.

———. 2017. Is Cyber Security Eating Internet Governance? Causes and Consequences of Alternative Framings. *Digital Policy, Regulation and Governance* 19(6): 415–28. https://doi.org/10.1108/DPRG-05-2017-0025.

Mustafa, Syed Ziaul, and Arpan Kumar Kar. 2019. Prioritization of Multi-dimensional Risk for Digital Services Using the Generalized Analytic Network Process. *Digital Policy, Regulation and Governance* 21(2): 146–63. https://doi.org/10.1108/DPRG-06-2018-0031.

National Association of State Chief Information Officers (NASCIO). 2014. *Deloitte-NASCIO Cyber Security Study*. Lexington, KY: NASCIO.

Nedovic-Budic, Zorica, and David Godschalk. 1996. Human Factors in Adoption of Geographic Information Systems: A Local Government Case Study. *Public Administration Review* 56(6): 554–67. https://doi.org/10.2307/977254.

New Zealand Government. 2015. New Zealand's Cyber Security Strategy. https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy [accessed May 7, 2020].

New Zealand Government. 2018. *National Cyber Policy Office Proactive Release*. April. https://dpmc.govt.nz/sites/default/files/2018-04/ers-18-paper-refresh-of-new-zealands-cyber-security-strategy-and-action-plan_1.pdf [accessed May 7, 2020].

Nichols, Shaun. 2019. A Stranger's TV Went on Spending Spree with My Amazon Account—and Web Giant Did Nothing about It for Months. *The Register*, October 31. https://www.theregister.co.uk/2019/10/31/amazon_account_hacking/ [accessed May 7, 2020].

Norris, Donald F., Anupam Joshi, and Tim Finin. 2015. Cybersecurity Challenges to American State and Local Governments. In *Proceedings of the 15th European Conference on eGovernment* 196–202. Portsmouth, UK: University of Portsmouth.

Norris, Donald F., and Kenneth L. Kraemer. 1996. Mainframe and PC Computing in American Cities: Myths and Realities. *Public Administration Review* 56(6): 568–76. https://doi.org/10.2307/977255.

Norris, Donald F., Laura Mateczun, Anupam Joshi, and Tim Finin. 2017. Cybersecurity Challenges to American Local Governments. Proceedings of 17th European Conference on Digital Government, 110–117.

———. 2018. Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security. *Journal of Homeland Security and Emergency Management* 15(3). https://doi.org/10.1515/jhsem-2017-0048.

———. 2019. Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review* 79(6): 895–904. https://doi.org/10.1111/puar.13028.

Norris, Donald F., and M. Jae Moon. 2005. Advancing E-Government at the Grassroots: Tortoise or Hare? *Public Administration Review* 65(1): 64–75. https://doi.org/10.1111/j.1540-6210.2005.00431.x.

Norris, Donald F., and Christopher G. Reddick. 2013. Local E-Government in the United States: Transformation or Incremental Change? *Public Administration Review* 73(1): 165–75. https://doi.org/10.1111/j.1540-6210.2012.02647.x.

Northrop, Alana, Kenneth L. Kraemer, Debora E. Dunkle, and John L. King. 1990. Payoffs from Computerization: Lessons over Time. *Public Administration Review* 50(5): 505–14. https://doi.org/10.2307/976781.

Nthala, Norbert, and Ivan Flechais. 2017. If It's Urgent or It Is Stopping Me from Doing Something, Then I Might Just Go Straight at It: A Study into Home Data Security Decisions. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* 123–42. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-58460-7_9.

Nye, Joseph S., Jr. 2010. *Cyber Power*. Harvard Kennedy School, Belfer Center for Science and International Affairs. May. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [accessed May 7, 2020].

Nye, Joseph S., Jr. 2011. Nuclear Lessons for Cyber Security. *Strategic Studies Quarterly* 5(4): 18–38.

———. 2014. The Regime Complex for Managing Global Cyber Activities. Paper Series: No. 1, Global Commission on Internet Governance. http://www.cigionline.org/publications/regime-complex-managingglobal-cyber-activities [accessed May 7, 2020].

———. 2015. *Power and Policy in an Information Age*. New York: PublicAffairs.

Okuku, Angela, Karen Renaud, and Brandon Valeriano. 2015. Cyber Security Strategy's Role in Raising Kenyan Awareness of Mobile Security Threats. *Information & Security: An International Journal* 32(1): 1–20. https://doi.org/10.11610/isij.3207.

Organisation for Economic Co-operation and Development (OECD). 2009. Financial Literacy and Consumer Protection: Overlooked Aspect of the Crisis. http://www.oecd.org/finance/financial-markets/43138294.pdf [accessed May 7, 2020].

Parshall, Joel. 2018. Cyberattacks Pose Increasing Industry Threat. *Journal of Petroleum Technology* 70(1): 36–7. https://doi.org/10.2118/0118-0036-JPT.

Petersen, Kim. 2018. Is China Neoliberal? Dissident Voice, March 7. https://dissidentvoice.org/2018/03/is-china-neoliberal/ [accessed May 7, 2020].

Phoenix, Jo, and Laura Kelly. 2013. "You Have to Do It for Yourself": Responsibilization in Youth Justice and Young People's Situated Knowledge of Youth Justice Practice. *British Journal of Criminology* 53(3): 419–37. https://doi.org/10.1093/bjc/azs078.

Pidgeon, Nick F., Christopher Hood, David K.C. Jones, Barry Turner, and R. Gibson. 1992. Risk Perception. In *Risk: Analysis, Perception and Management: Report of a Royal Society Study Group* 89–134. London: Royal Society.

PONEMON Institute. 2018. *Cost of a Data Breach Study: Global Overview*. Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC.

Poole, Erika Shehan, Marshina Chetty, Tom Morgan, Rebecca E. Grinter, and W. Keith Edwards. 2009. Computer Help at Home: Methods and Motivations for Informal Technical Support. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 739–748). New York: ACM. https://doi.org/10.1145/1518701.1518816

Public Safety Canada. 2018. National Cyber Security Strategy. https://www.canada.ca/en/public-safety-canada/news/2018/06/national-cyber-security-strategy.html [accessed May 7, 2020].

Quigley, Kevin, and Jeffrey Roy. 2012. Cyber-Security and Risk Management in an Interoperable World: An Examination of Governmental Action in North America. *Social Science Computer Review* 30(1): 83–94. https://doi.org/10.1177/0894439310392197.

Renaud, Karen, and George R. S. Weir. 2016. Cybersecurity and the Unbearability of Uncertainty. In *Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC)*. https://doi.org/10.1109/CCC.2016.29.

Renaud, Karen, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. 2018. Is the Responsibilization of the Cyber Security Risk Reasonable

and Judicious? *Computers & Security* 78: 198–211. https://doi.org/10.1016/j.cose.2018.06.006.

Rid, Thomas. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies* 35(1): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Rossiter, Katherine. 2012. Talking Turkey: Anxiety, Public Health Stories, and the Responsibilization of Health. *Journal of Canadian Studies* 46(2): 178–95. muse.jhu.edu/article/515018.

Schulzke, Marcus. 2018. The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. *Perspectives on Politics* 16(4): 954–68. https://doi.org/10.1017/S153759271800110X.

Selby, James. 2019. Louisiana Victim Scammed Online for over $22k by Man in U.S. on Expired Visa. October 16. https://www.myarklamiss.com/news/crime-news/louisiana-victim-scammed-online-for-over-22k-by-man-in-u-s-on-expired-visa/ [accessed May 7, 2020].

Senol, Mustafa. 2017. An Approach for Creation and Implementation of National Cyber Security Strategy. In *International Conference on Computer Science and Engineering (UBMK)*, 189–194. https://doi.org/10.1109/UBMK.2017.8093373.

Shackelford, Scott, and Amanda Craig. 2014. Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber Security. *Stanford Journal of International Law* 50: 119–52.

Shamir, Ronen. 2018. The Age of Responsibilization: On Market-Embedded Morality. *Economy and Society* 37(1): 1–19. https://doi.org/10.1080/03085140701760833.

Shrouf, Fadi, and Giovanni Miragliotta. 2015. Energy Management Based on Internet of Things: Practices and Framework for Adoption in Production Management. *Journal of Cleaner Production* 100: 235–46. https://doi.org/10.1016/j.jclepro.2015.03.055.

Singh, Abhishek Narain, Arnold Picot, Kranz Johann, M.P. Gupta, and Amitabh Ojha. 2013. Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management* 14(4): 225–39. https://doi.org/10.1007/s40171-013-0047-4.

Skinns, Layla. 2003. Responsibility, Rhetoric and Reality: Practitioners' Views on Their Responsibility for Crime and Disorder in the Community Safety Partnerships. In *British Society of Criminology*. http://www.britsoccrim.org/volume6/007.pdf [accessed May 7, 2020].

Soneryd, Linda, and Ylva Uggla. 2015. Green Governmentality and Responsibilization: New Forms of Governance and Responses to "Consumer Responsibility". *Environmental Politics* 24(6): 913–31. https://doi.org/10.1080/09644016.2015.1055885.

Standford, Jim. 2014. *Canada's Transformation under Neoliberalism*. Canadian Dimension, March 29. https://canadiandimension.com/articles/view/canadas [accessed May 7, 2020].

Stol, Yrrah H., Maartje H. Schermer, and Eva C.A. Asscher. 2016. Omnipresent Health Checks May Result in Over-Responsibilization. *Public Health Ethics* 10(1): 35–48. https://doi.org/10.1093/phe/phw034.

Tossini, J. Vitor. 2017. The Five Eyes—The Intelligence Alliance of the Anglosphere. *UK Defence Journal*, November 14. https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere [accessed May 7, 2020].

Tsinovoi, Alexei, and Rebecca Adler-Nissen. 2018. Inversion of the "Duty of Care": Diplomacy and the Protection of Citizens Abroad, from Pastoral Care to Neoliberal Governmentality. *Hague Journal of Diplomacy* 13(2): 1–22. https://doi.org/10.1163/1871191X-11302017.

U.S. Information Technology Office (USITO). 2016. China Publishes First National Cyber Security Policy. December 27. http://www.usito.org/news/china-publishes-first-national-cyber security-strategy [accessed May 7, 2020].

Valeriano, Brandon, and Ryan Maness. 2018. International Political Theory and Cyber Security. In *The Handbook of International Political Theory*, edited by Chris Brown and Robyn Eckersley, 259–72. Oxford: Oxford University Press.

Väljataga, Ann. 2018. Tracing *opinio juris* in National Cyber Security Strategy Documents. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/library/publications/tracing-opinio-juris-in-national-cyber-security-strategy-documents/ [accessed May 7, 2020].

Schaik, van, Joseph Onibokun Paul, Jean Camp, Jurjen Jansen, and Petko Kusev. 2018. Security and Privacy in Online Social Networking: Risk Perceptions and Precautionary Behavior. *Computers in Human Behavior* 78: 283–97. https://doi.org/10.1016/j.chb.2017.10.007.

Ventura, Stephen J. 1995. The Use of Geographic Information Systems in Local Government. *Public Administration Review* 55(5): 461–7. https://doi.org/10.2307/976770.

Wakefield, Alison, and Jenny Fleming. 2008. *The Sage Dictionary of Policing*. London: Sage Publications.

Wang, Amy B. 2018. **"**I'm in Your Baby's Room": A Hacker Took over a Baby Monitor and Broadcast Threats, Parents Say. *Washington Post*, December 20. https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/ [accessed May 7, 2020].

Weeks, John. 2005. Inequality Trends in Some Developed OECD Countries. Working Paper 6, United Nations Department of Economic and Statistical Affairs. http://www.un.org/esa/desa/papers/2005/wp6_2005.pdf [accessed May 7, 2020].

West, Darrell M. 2004. E-Government and the Transformation of Service Delivery and Citizen Attitudes. *Public Administration Review* 64(1): 15–28. https://doi.org/10.1111/j.1540-6210.2004.00343.x.

White House. 2018. National Cyber Strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [accessed May 7, 2020].

Wiemann, Gabriel. 2006. *Cyberterrorism: How Real Is the Threat?* Special Report. United States Institute of Peace, May 13. https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat [accessed May 7, 2020].

Williams, Dan. 2019. *Israeli Cyber-Hotline Offers Help for the Hacked*. Reuters, February 18. https://www.reuters.com/article/us-cyber-israel-hotline-idUSKCN1Q70K1 [accessed May 7, 2020].

World Economic Forum. 2018. The Global Risks Report 2018. https://www.weforum.org/reports/the-global-risks-report-2018 [accessed May 7, 2020].

WTVR. 2019. Man from Ghana Duped Virginia Woman out of $300K in Online Romance Scam, Feds Say. October 3. https://wtvr.com/2019/10/03/man-from-ghana-swindles-virginia-woman-out-of-300000-feds-say/ [accessed May 7, 2020].

Xavier, Umesh Hodeghatta Rao, and Bishwa Prakash Pati. 2012. Study of Internet security threats among home users. In *Fourth International Conference on Computational Aspects of Social Networks* (CASoN), 217–221. New York: IEEE. http://doi.org/10.1109/CASoN.2012.6412405.

Zhao, Jensen J., and Sherry Y. Zhao. 2010. Opportunities and Threats: A Security Assessment of State E-Government Websites. *Government Information Quarterly* 27(1): 49–56. https://doi.org/10.1016/j.giq.2009.07.004.

Zhu, Jiangnan, Huang Huang, and Zhang Dong. 2019. Big Tigers, Big Data: Learning Social Reactions to China's Anticorruption Campaign through Online Feedback. *Public Administration Review* 79(4): 500–13. https://doi.org/10.1111/puar.12866.

Supporting Information

A supplementary appendix may be found in the online version of this article at http://onlinelibrary.wiley.com/doi/10.1111/puar.13210/full.